Sprint Corporation
Mailstop VARESA0209
12502 Sunrise Valley Drive
Reston, VA 20196
Office: (703) 592-7580
Fax: (703) 433-4084

Maureen Cooney
Head of Privacy
Office of Privacy
maureen.cooney@sprint.com

Electronic Filing via ECFS

Executed on: February 28, 2018
Date filed: March 1, 2018

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

Re: Annual CPNI Compliance Certification, EB Docket No. 06-36

Dear Secretary Dortch:

Attached, for filing in EB Docket No. 06-36, is the annual 47 C.F.R. § 64.2009(e) CPNI Compliance Certification and accompanying statement of Sprint Corporation.

If there are any questions regarding this filing, please contact the undersigned. Thank you for your assistance.

Respectfully submitted,

Maureen Cooney
Head of Privacy – Office of Privacy
Sprint Corporation

Sprint Corporation
900 7th Street, NW
Washington, DC 20001
Office: (202) 585-1902
Fax: (202) 585-1940

Vonya B. McCann
Senior Vice President
Government Affairs
vonya.b.mccann@sprint.com

Annual 47 C.F.R. §64.2009(e) CPNI Certification
EB Docket 06-36

Date Filed: March 1, 2018

Name of company covered by this certification: Sprint Corporation

Form 499 Filer ID:
804636 – Sprint Communications Company LP
804639 – US Telecom, Inc.
811754 – Sprint Spectrum LP / Phillieco LP (dba Sprint PCS)
822596 – Virgin Mobile USA, LP

Name of Signatory: Vonya B. McCann
Title of Signatory: Senior Vice President -- Government Affairs

SPRINT CORPORATION
2017 CPNI COMPLIANCE CERTIFICATE AND STATEMENT

I, Vonya B. McCann, certify that I am an officer of Sprint Corporation, and I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules (see 47 C.F.R. § 64.2001 *et seq.*).

Attached to this certification is a statement explaining how the company's operating procedures ensure compliance with the requirements of section 64.2001 et seq. of the Commission's rules. The statement also provides a summary of the customer complaints that the company has received in the past year concerning the unauthorized access to CPNI. As explained more fully in the accompanying statement, Sprint has not taken any actions against any data brokers in the past year.

The company represents and warrants that the certification is consistent with 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Executed on February 26, 2018

Vonya B. McCann
Senior Vice President – Government Affairs
Sprint Corporation

Attachment: Accompanying statement

SPRINT CORPORATION
ATTACHMENT A
2017 CPNI Compliance Statement of Operating Procedures

The following statement explains the operating procedures established by Sprint Corporation and its affiliates (collectively, "Sprint" or "Company") to ensure that it is in compliance with the Federal Communications Commission's ("FCC" or "Commission") Customer Proprietary Network Information ("CPNI") rules.[1] Specifically, "Sprint" refers to all of Sprint Corporation's operating entities and divisions, including those referred to as Sprint, Boost Mobile, and Virgin Mobile USA, L.P. (including Assurance Wireless).[2]

Sprint's Office of Privacy, along with several business units, monitors the Company's systems and processes related to its enterprise-wide CPNI compliance programs. As such, Sprint will continue to update and deploy CPNI training; review and adjust, where necessary, its customer authentication, information security, and notification procedures; and strengthen the Company's administrative, physical and technical safeguards.

Safeguards

Sprint takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. As such, Sprint employs administrative, physical and technical safeguards that are designed to protect CPNI from unauthorized access, use and disclosure.

Sprint limits CPNI access to employees, independent contractors and joint venture partners consistent with their job functions. If access is required, they must first obtain approval through established administrative processes. Once approval is granted, user ID's and passwords are issued. Access credentials are governed by Sprint's corporate security policies, which are consistent with industry standard requirements for password management for information technology networks, applications and databases.

Before disclosing CPNI to independent contractors or joint venture partners, Sprint enters into agreements with strict privacy and confidentiality provisions that require third parties to maintain confidentiality, protect the information, and comply with the law. Sprint's Office of Privacy continually reviews Sprint's standard privacy-related contract terms and conditions to ensure that those provisions adequately safeguard all customer information. In negotiating and renewing its contracts, Sprint requires independent contractors and joint venture partners with which it shares CPNI to safeguard this information in a manner that is consistent with the FCC's rules. Specifically, these contract terms require third parties with access to CPNI to have appropriate CPNI protections in place to ensure the ongoing confidentiality of such information. These provisions require securing all CPNI, limiting access to persons who have a need-to-know such information in connection with the performance of the contract, ensuring all persons with access are bound by specified confidentiality obligations, restricting the use of CPNI solely to the performance of the contract, and securely returning or destroying CPNI when it is no longer necessary to perform the functions for which it was provided.

Permitted Uses of CPNI without Customer Approval

Sprint may use CPNI in certain circumstances that do not require customer approval, in accordance with Section 222 of the Communications Act, as amended, and the Commission's rules. Such uses may include, but are not limited to, providing or marketing services within the customer's total service relationship, provisioning customer premises equipment (CPE), and protecting Sprint's rights and property, as well as protecting users of its services from fraudulent, abusive, or unlawful use of, or subscription to, such services.

Review and Recordkeeping for CPNI Marketing Use and Sharing

Sprint uses a marketing campaign management system for review, approval and recordkeeping for outbound marketing campaigns that involve the access, use or disclosure of CPNI. Sprint's supervisory review process helps to ensure that Sprint does not use the CPNI in a way that violates the CPNI rules.

---

[1] This statement does not cover CPNI derived from Sprint's Telecommunications Relay Services ("TRS"). Sprint will file a separate certification for TRS in accordance with 47 C.F.R. §64.5109(e).

[2] Boost Mobile, LLC ("Boost") and Virgin Mobile USA, L.P. ("Virgin Mobile") are subsidiaries of Sprint Corporation.

Records of all the foregoing marketing campaign activities are maintained through the use of marketing resource and project management tools. A description of the campaign and details on what products and services are offered in the campaign are maintained in Sprint's marketing resource management tool. Any marketing campaign that uses CPNI is identified as such in the marketing campaign management system.

CPNI Notice and Consent Process

Sprint uses CPNI to provide customers with the services to which they subscribe and for marketing purposes within the total service relationship. Sprint has processes, procedures and operational controls in place to prevent access, use and disclosure of CPNI for marketing services to which the customer does not already subscribe (i.e., cross-marketing). As such, Sprint does not send out CPNI opt-out notices.

Sprint also has processes, procedures and operational controls in place to prevent access, use and disclosure of CPNI for marketing of non-communications related products or services and, thus, does not obtain opt-in consent for those purposes. If, in the future, Sprint uses CPNI for cross-marketing or non-communications purposes, Sprint will first send opt-out notices or obtain the appropriate opt-in consent as required by the CPNI rules.

Training and Disciplinary Process

Consistent with Sprint's commitment to preserving customer privacy, the Company is continuing with a variety of training programs for its employees and contractors. The training explains how Sprint employees and contractors must access, use, store, disclose and secure CPNI to ensure compliance with the FCC's rules and Company policies. In 2017, all employees and all contractors who had access to CPNI took CPNI training.

Sprint also maintains a disciplinary process as part of Company procedures that addresses CPNI compliance. Sprint security personnel investigate instances of potential improper access or disclosure of CPNI by employees. If the investigation indicates a violation has occurred, disciplinary action is taken, up to and including termination.

Authentication

Through Sprint's billing platform, Sprint wireless customers establish a Personal Identification Number (PIN) that is required for account access to sensitive customer information. The billing platform also allows customers to pre-select a security question and provide an answer to that question as a back-up authentication method for when a customer cannot recall his/her PIN. Customers may also access their account online using their online user ID and password or by visiting a retail location and providing a valid government issued photo ID. Where appropriate, and as permitted by the Commission's rules, Sprint may work directly with a business customer through a dedicated representative to establish an authentication regime that works best for that customer. Customers are not authenticated using readily available biographical information or account information when attempting to access call detail records over the telephone or when establishing or changing their PIN.

Sprint wireless customers who wish to obtain their call detail information have several options. Sprint encourages customers to access their call detail records by logging in to their sprint.com account. Alternatively, if contacting Sprint by telephone, Sprint will send call detail records only after the customer has been authenticated using his/her PIN or answer to a pre-selected security question. Customers with a valid, government issued photo ID also may visit a Sprint retail store to establish or change his/her account PIN or to access call detail records.

For wireless customers who wish to access their account online, Sprint requires all customers to establish

and use an online username and password. Prior to establishing an online username and password, Sprint authenticates these customers by verifying their pre-established PIN or security question. If such credentials are not known, a Customer may elect to create a limited access level profile by retrieving an SMS with a temporary verification code to his/her wireless device and entering that code to create a limited access online account. If the customer cannot recall his/her online username or password, Sprint makes several backup methods available so that those customers can be authenticated before they retrieve their information. For wireless customers who wish to view account information through Sprint's self-service mobile app feature, Sprint authenticates the customer's device at the network level, and requires customers to use their online username and password depending on the account information to be accessed.

For wireline customers, Sprint has compliant processes to handle customers who contact Sprint via telephone. If a wireline customer requests access to his/her call detail records, Sprint will only send those records to the address confirmed with the customer or via a follow-up outbound call to the customer's telephone number of record, as defined by the CPNI rules.

Notifications

Sprint provides notice to its customers when a triggering event occurs. Such events include the creation of, or change to, an account PIN, password, security question or answer, online account, or address of record. These notifications are provided to customers through a variety of means, including messages to the customer's telephone number of record, postal mail or electronic mail to the customer's address of record, and SMS messages. The notification includes information to alert the customer of the underlying event, but does not disclose any of the new or changed information, in accordance with the FCC's rules.

In the event that a breach of customer information includes CPNI, Sprint provides notice to law enforcement. In accordance with the Commission's rules, Sprint provides notice to impacted customers after completing the process of notifying law enforcement. Such notification provides customers with enough information to understand the nature of the breach, the scope of impacted information and recommendations on how the customer should respond. If the impacted customer alerts Sprint of a potential breach, Sprint investigates the customer's allegations and communicates as necessary with the customer and/or law enforcement.

Data Brokers

In 2017, Sprint did not detect pretexting activities by data brokers. Therefore, Sprint did not institute any proceedings or file any petitions against any data broker in any state commission, the court system or the FCC. Sprint continues to deploy safeguards to protect against, detect, and mitigate pretexting activities.

CPNI Complaint Reporting

Sprint's CPNI compliance program includes processes that enable Sprint to comply with CPNI documentation and reporting obligations, including maintaining a record of notifications to, and responses from, law enforcement and customers, and the relevant dates and descriptions of the complaints. These records are maintained for a minimum of two years.

The following data is comprised of all complaints related to unauthorized access received by Sprint in 2017. Some of these complaints were submitted to Sprint directly by the complainants themselves, and some have been called to Sprint's attention by government agencies or the Better Business Bureau.

The complaints are broken down by category, as follows:

- Number of complaints of alleged unauthorized access to CPNI by a third party: 27 (substantiated: 0)

- Number of complaints of alleged unauthorized access to CPNI by a Sprint employee or contractor: 10 (substantiated: 5)

- Number of complaints of alleged unauthorized online access to CPNI: 65 (substantiated: 1)

Sprint investigates all of these complaints. These investigations show that in many of the cases there is no evidence that a CPNI violation occurred. As for the remaining cases, if Sprint confirms a violation, or determines that there is evidence of a violation, Sprint classifies the complaint as one implicating CPNI.

Conclusion

Sprint, through its Office of Privacy and other business units, monitors the Company's policies and procedures to ensure continued compliance with the FCC's CPNI regulations.